Laporan Dwi Bulan I 2014

ID-CERT[1]

Ringkasan

Di Laporan Dwi Bulan I 2014 ini disajikan hasil pengumpulan pengaduan selama dua bulan yaitu Januari dan Februari 2014. Pengaduan tersebut diterima dalam bentuk email dan dikumpulkan sesuai kategori, sebagai bahan penyusunan statistik, dalam bentuk angka dan grafik. Spam, komplain spam, respon, network incident, Hak atas Kekayaan Intelektual, fraud, spoofing/phising, dan malware merupakan kategori yang dipilih untuk pengelompokan pengaduan masuk.

Kata Kunci
Security – Pelaporan - Laporan Dwi Bulan

Daftar isi

1. Pendahuluan

Bagian penting dari aktivitas sekarang adalah Internet. Pemakaian Internet sehari-hari kian menjadi lebih penting dari komunikasi antarwarga hingga transaksi bisnis multinasional, pengguna Internet kian banyak dan kian beragam – usia kanak-kanak sampai dengan para lansia, para pekerja di lapangan hingga *bot otomatis*. Batas-batas yang telah ada sebelumnya juga mengalami pergeseran dengan adanya Internet, menciptakan kemungkinan baru yang perlu dicermati. Tidak terkecuali aspek keamanan Internet (*Internet security*) yang menjadi perhatian secara khusus dan kerja sama banyak kalangan.

Sebagai bagian dari pemantauan keamanan Internet, ID-CERT[1] menerima pengaduan lewat e-mail yang diterima dari beberapa responden. Pengaduan tersebut dikelompokkan dalam sejumlah kategori dan disajikan dalam bentuk laporan Dwi Bulan. Laporan ini sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi selama dua bulan, Januari dan Februari 2014.

[1] Indonesian Computer Emergency Respons Team

Selain gambaran tersebut, penyediaan laporan ini juga dimaksudkan sebagai contoh data primer keamanan teknologi informasi (TI) di Indonesia.
Penting ditekankan dalam hal ini adalah tindak lanjut terhadap laporan tentang penyalah gunaan Internet (*Internet abuse*) sebagai respon positif dan langkah untuk memperbaiki keadaan. Hal ini juga bagian interaksi positif antara kita, pengguna Internet di Indonesia dengan pihak-pihak di mancanegara terkait penanganan laporan. Pengaduan yang diterima memberi gambaran bagian-bagian yang perlu dibenahi, keterkaitan antar lembaga, dan untuk membantu penyusunan rencana ke depan.
Pada laporan Dwi Bulanan I 2014 ini spam masih menempati jumlah pengaduan terbanyak yaitu mencapai 67%, jumlah tersebut lebih dari empat kalinya malware yang menempati urutan pengaduan ke dua yaitu sebesar 11%. Fenomena lainnya adalah penurunan jumlah pengaduan dari Januari ke Februari 2014.
Dilihat dari sisi jumlah pengaduan, terdapat tiga kelompok besar: spam sendiri pada kelompok pertama yang mencapai jumlah di atas 12.000 pengaduan, dikuti kelompok ke dua yang memiliki jumlah pelaporan sedang yaitu di bawah 4.000 di atas 2.000 laporan, dan kelompok terakhir berjumlah pengaduan rendah yaitu di bawah 2.000 pengaduan. Penjelasan lengkap tentang ketiga kelompok tersebut dipaparkan di bagian Uraian.
Pembuatan laporan ini berdasarkan pada data-data yang diperoleh dan diambil dari tiga puluh tujuh (37) responden yang terdiri dari: Kominfo, ID-CERT, PANDI, Detik.net, Zone-h dan Anti Fraud Command Center (AFCC), tiga operator telekomunikasi, tujuh NAP, dan 22 Penyedia Jasa Internet (PJI/ISP)

2. Metoda

Penyusunan dokumen Dwi Bulan ini mengambil data dari beberapa sumber dalam bentuk laporan dengan langkah-langkah berikut :

1. Pengambilan data dari sejumlah responden.
2. Penyusunan analisis berdasarkan :

a) Tembusan laporan yang masuk lewat alamat e-mail pengaduan penyalahgunaan (*abuse*) yang disediakan PJI/operator telekomunikasi/lembaga non-ISP.
b) Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi ini berupa kumpulan data yang telah dihitung dan dikelompok-kan oleh responden.

Dari laporan yang sudah terkumpul, dilakukan pengelompokan sebagai berikut :

Fraud Penipuan disengaja yang dibuat untuk keuntungan pribadi atau untuk merugikan individu lain[2] berdasarkan data yang sudah masuk ke penegak hukum.

Hak atas Kekayaan Intelektual Pengaduan tentang pelanggaran terhadap hasil karya yang terkait Undang Undang Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR).

Komplain Spam Keluhan/pengaduan e-mail spam dari dalam negeri terhadap pengirim di Indonesia dan luar negeri.

Malware Program komputer yang dibuat untuk maksud jahat[3].

Network Incident Aktivitas yang dilakukan terhadap jaringan pihak laindan semua aktivitas terkait dengan penyalahgunaan jaringan.

Respon Respon terhadap laporan yang masuk.

Spam Penggunaan sistem pengolahan pesan elektronik untuk mengirim pesan-pesan tidak diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih[4].

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna[5].

Lain-lain Laporan penyalahgunaan selain yang termasuk pada kategori yang di atas.

---

[2] *Fraud*, http://en.wikipedia.org/wiki/Fraud
[3] *Malware*, http://en.wikipedia.org/wiki/Malware
[4] *Spam (electronic)*, http://en.wikipedia.org/wiki/Spam_(electronic)
[5] *Spoofing attack*, http://en.wikipedia.org/wiki/Spoofing_attack

3. Uraian

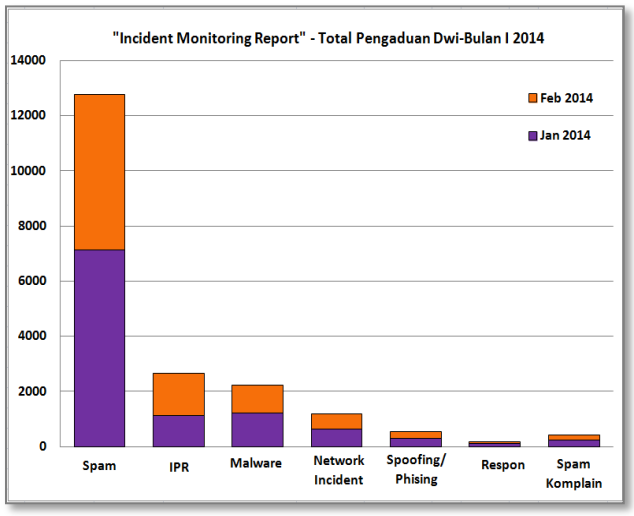
Email pengaduan yang diterima dikumpulkan berdasarkan kategori pengaduan dan bulan, dengan demikian terdapat dua kelompok besar, bulan Januari dan Februari 2014. Kategori pengaduan terdiri atas Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Proprty Rights* (IPR), komplain spam, *malware*, *network incident*, respon, *spam*, dan *spoof*. Pengolahan data dilakukan dengan dua cara :

1. Penghitungan cacah dari tajuk (header) email, seperti bagian `From`, `To`, `CC`, dan `Subject`. Cara ini terutama digunakan untuk pengaduan dalam kondisi tidak terformat bagus, karena email tidak mengikuti format baku yang biasanya dihasilkan perangkat lunak pelapor. Kategori pengaduan seperti spam, spoof biasanya termasuk jenis ini.
2. Penghitungan cacah dari isi email (body). Pengaduan network incident dan malware sebagai misal, menggunakan format pesan yang baku dan nama domain yang diadukan dapat diperoleh dari isi email pada bagian yang menggunakan format tertentu.

Grafik semua kategori Incident Monitoring Report untuk Dwi Bulan I 2014 berdasarkan jumlah pengaduan per bulan ditampilkan pada Gambar 1.

Jumlah pengaduan masing-masing dapat dilihat lebih seksama di Tabel 1 dengan kategori pengaduan ditampilkan berdasarkan urutan abjad. Perhitungan perkembangan dilakukan terhadap jumlah pengaduan pada bulan pertama, Januari dan bernilai negatif jika terjadi penurunan. Secara umum terjadi penurunan jumlah pengaduan Februari di banding Januari kecuali IPR yang justru terjadi peningkatan pengaduan sehingga mencapai kenaikan sebesar 39,1%.

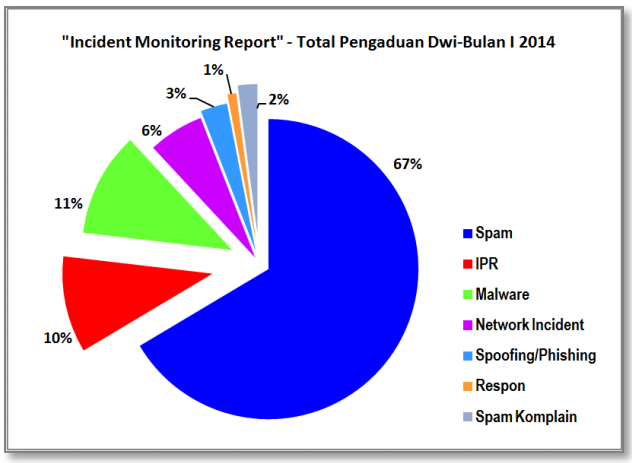
Total pengaduan selama dua bulan dan persentase masing-masing dihitung terhadap jumlah pengaduan keseluruhan dapat dilihat pada Tabel 2. Tampilan tabel tersebut berdasarkan urutan persentase kategori dari terbanyak. Tampilan dalam bentuk diagram lingkaran disajikan pada Gambar 2.



Gambar 1. Incident Monitoring Report Dwi Bulan I 2014 untuk semua kategori.

Kategori	Januari	Februari	Perkembangan
IPR	1,115	1,551	39.1 %
Komplain Spam	226	176	- 22.1 %
Malware	1,205	1,024	- 15.0 %
Network Incident	640	553	- 13.6 %
Spam	7,115	5,639	- 20.7 %
Spoof	307	242	- 21.2 %

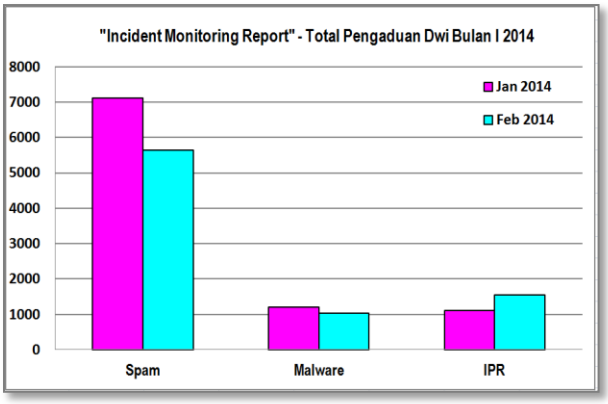
Tabel 1. Perkembangan jenis pengaduan selama Januari dan Februari 2014



Gambar 2. Persentase pengaduan per kategori Dwi Bulan I 2014.

3.1. *Spam, IPR,* dan *malware*

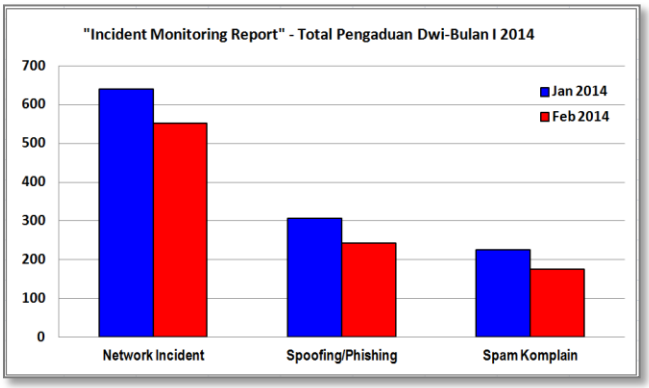
Pada periode Januari – Februari 2014 ini jumlah pengaduan terbanyak adalah kategori *spam* dengan jumlah 12.754 atau 64,44% dari total pengaduan. Dengan jumlah lebih dari separuh pengaduan, *spam* mendominasi pengaduan dan terlihat pada angka tersebut yang di atas lima kali dari kategori di bawahnya yaitu *IPR.*
Terjadi penurunan jumlah pengaduan dari bulan Januari ke Februari 2014, *spam* 20,7% dan *malware* 15,0% sedangkan *IPR* terjadi kenaikan sebesar 39,1%. Terlihat perbedaan yang cukup mencolok pada jumlah pengaduan *spam* yang menduduki peringkat pertama, *IPR* peringkat kedua walaupun mengalami peningkatan dan *malware* pada peringkat ketiga disajikan pada Gambar 3.



Gambar 3. Perkembangan jumlah pengaduan *spam*, *malware*, dan *IPR*.

3.2. Network incident, spoofing/ phising, dan komplain spam

Kelompok kedua pengaduan diawali oleh *network incident* dengan total pengaduan 1.193 atau 6,03%, diikuti oleh *spoofing/phising* dengan jumlah pengaduan 549 atau 2,7%, dan terakhir spam komplain dengan jumlah pengaduan 402 atau 2,0% ditampilkan dalam Gambar 4.
Jika dilihat dari pesan pengaduan yang diterima, pengaduan ini diterima dari pelaporan non-otomatis, yakni pengaduan yang dikirim oleh pengguna komputer (bukan dari perangkat lunak atau alat bantu).



Gambar 4. Jumlah pengaduan *network incident*, *spoofing/phising*, dan *spam* komplain Januari-Februari 2014

Dari beberapa kemungkinan akan fenomena di atas, dua hal perlu dipertimbangkan :

1. Pengguna Internet "menyelesaikan sendiri" urusan spam, baik menggunakan fasilitas pelaporan yang sudah disediakan layanan (sebagai misal hampir semualayanan email berbasis web sudah menyediakan penandaan "pesan sebagai spam") atau membiarkan spam ini dengan cukup menghapusnya.
2. ID-CERT perlu terus merangkul pihak-pihak lain untuk sosialisasi mekanisme pengaduan agar dapat menjaring lebih banyak laporan.

4. Rangkuman

Dengan pertimbangan jumlah pengaduan spam masih tertinggi, perlu menjadi perhatian para administrator jaringan, baik untuk jaringan lokal atau jaringan di bawah layanan Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi "pintu gerbang" pengiriman spam (terutama lewat email) dan mengantisipasi kedatangan spam.
Dua bulan pertama ini, Januari dan Februari, jumlah pengaduan spam sangat dominan dibanding kategori lainnya dan terjadi penurunan pada bulan kedua.
Dilihat dari volume pengaduan yang masuk, yang menggambarkan kepedulian para pelapor terhadap isu keamanan Internet – menjadi tanggung jawab pihak-pihak terkait dengan

bahan laporan tersebut untuk menindaklanjuti dalam bentuk respon atau aksi yang diperlukan. Dengan demikian prosedur standar yang menjadi acuan dapat dijalankan dengan baik dan kepercayaan pihak pelapor terjaga atau meningkat.

4.1. Rekomendasi

Sejumlah rekomendasi yang dapat dipertimbangkan :

1. Perangakat lunak anti-spam dipasang di server email sebagai antisipasi pengiriman pesan spam dari jaringan lokan ke Internet.
2. Perangakat lunak anti virus dan perangkat lunak keamanan dipasang untuk mengurangi resiko terinfeksi malware. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara tertatur.
3. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, misalnya akses ke port email/Postfix[6] secara intensif dalam periode lama atau berulang-ulang.
4. Administrator jaringan memblokir semua port akses ke Internet, kecuali untuk port yang dianggap diperlukan.
5. Penyedia Jasa Internet (PJI/ISP) dan operator telekomunikasi disarankan menyediakan tombol pelaporan khusus penyalahgunaan Internet (Internet abuse) guna kemudahan pelaporan.
6. Formulir pengaduan penyalahgunaan Internet (Internet abuse) dicantumkan di setiap situs web.
7. Terkait Hak atas Kekayaan Intelektual (HaKI), sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai materi (content) yang dianggap melanggar HaKI, karena PJI atau penyedia materi memerlukan landasan hukum yang jelas untuk menurunkan materi yang bermasalah.
8. Semua pihak wajib menindaklanjuti setiap laporan kaluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada penegak hukum.

5. Ucapan Terima Kasih

Laporan ini bisa disajikan karena adanya partisipasi dari beberapa pihak dalam hal pengumpulan bahan untuk penulisan laporan ID-CERT, yakni :

1. Kementrian Komunikasi dan Informatika (Kominfo)
2. Pengelola Nama Domain Internet Indonesia (PANDI)
3. Asosiasi Penyelenggaraan Jasa Internet Indonesia (APJII)
4. Detik (detik.net)
5. Tiga operator
   dan dua puluh dua PJI/ISP

6. Lampiran

6.1. Advanced Persistent Threat

Advanced Persistent Threat (APT) adalah serangkaian proses hacking yang tersembunyi dan berkesinambungan yang sering diatur oleh manusia yang menargetkan entitas tertentu. APT biasanya menargetkan organisasi dan atau negara untuk motif bisnis atau politik. Proses APT membutuhkan kerahasiaan tingkat tinggi selama jangka waktu yang panjang. Seperti namanya, APT terdiri dari tiga komponen utama/proses: advanced, gigih, dan ancaman. Proses advanced menandakan teknik canggih yang menggunakan malware untuk mengeksploitasi kerentanan dalam sistem. Proses yang gigih menunjukkan bahwa perintah dan kontrol eksternal terus-menerus memantau/ memonitor dan menggali data dari target tertentu. Proses ancaman mengindikasikan keterlibatan manusia dalam merancang serangan itu.

APT biasanya mengacu pada satu kelompok, seperti pemerintah dengan kemampuan dan niat untuk secara terus-menerus dan efektif menargetkan entitas tertentu.

[6] Posfix adalahperangkat lunak server email atau dikenal dengan Mail Transfer Agent (MTA) dan berdasarkan perhitungan tahun 2012 disebut digunakan oleh 23% server email di Internet.
Sumber: Wikipedia, http://en.wikipedia.org/wiki/Postfix_(software)

Istilah ini umumnya digunakan untuk merujuk kepada ancaman *cyber*, khususnya spionase internet yang menggunakan berbagai teknik pengumpulan intelijen untuk mengakses informasi sensitif, tetapi berlaku sama terhadap ancaman lain seperti spionase atau serangan tradisional. Vektor serangan yang dikenal lainnya termasuk media yang terinfeksi, meng-hack rantai *supply*, dan *social engineering*. Para Individu, seperti hacker perorangan, biasanya tidak disebut sebagai APT karena mereka jarang memiliki sumber daya yang advanced dan gigih bahkan jika mereka berniat mendapatkan akses ke, atau menyerang target tertentu.

1. History dan target

Peringatan pertama, pada email-email yang ditarget dan tersocial-engineering yang mengandung trojan untuk *exfiltrate* (mengambil) informasi sensitif, diterbitkan oleh organisasi Inggris dan US CERT pada tahun 2005, meskipun nama " APT " tidak digunakan. Istilah " ***Advanced Persistent Threat*** " secara luas disebut berasal dari Angkatan Udara pada tahun 2006 dengan Kolonel Greg Rattray yang sering disebut sebagai individu yang menciptakan istilah tersebut.

The Stuxnet computer worm, yang menarget-kan perangkat keras komputer dari program nuklir Iran, adalah salah satu contohnya. Dalam hal ini, pemerintah Iran mungkin mempertim-bangkan si pencipta Stuxnet sebagai advanced persistent threat.

Dalam komunitas keamanan komputer, dan dalam media, istilah ini hampir selalu digunakan dalam referensi untuk pola jangka panjang dari serangan hacking canggih yang ditujukan pada pemerintah, perusahaan, dan aktivis politik, dan juga untuk merujuk pada kelompok-kelompok di belakang serangan-serangan tersebut. *Advanced Persistent Threat* (APT) sebagai suatu istilah dapat mengalihkan fokus ke hack komputer karena meningkatnya jumlah kejadian. PC World melaporkan 81 persen kenaikan dari 2010 ke 2011 khususnya pada serangan hack komputer .

Kesalahpahaman umum yang terkait dengan APT adalah bahwa APT hanya menarget pemerintah Barat. Sementara contoh teknologi APT melawan pemerintah Barat lebih dipublikasikan di Barat, pelaku di banyak negara telah menggunakan dunia maya sebagai sarana untuk mengumpulkan intelijen pada individu dan kelompok individu. Cyber Command Amerika Serikat bertugas mengkoordinasikan respon militer AS terhadap ancaman dunia maya ini.

Banyak sumber telah menyatakan bahwa beberapa kelompok APT berafiliasi dengan, atau agen dari, negara bagian. Bisnis memegang sejumlah besar informasi pribadi yang beresiko tinggi menjadi target *Advanced Persistent Threat*, termasuk:

- Pendidikan tinggi
- Lembaga keuangan

2. Karakteristik APT

Bodmer , Kilger , Carpenter dan Jones mende-finisikan kriteria APT sebagai berikut :

- **Tujuan** – Tujuan akhir dari ancaman, musuh
- **Ketepatan waktu** – Waktu yang dihabiskan memasuki dan mengakses sistem
- **Sumber** – Tingkat pengetahuan dan peralatan yang digunakan dalam kejadian (serangan) tersebut (keterampilan dan metode akan menjadi titik utama)
- **Toleransi Risiko** - ancaman akan tetap tidak terdeteksi
- **Keterampilan dan metode** - Alat-alat dan teknik yang digunakan selama kejadian (serangan)
- **Tindakan** - Tindakan yang tepat dari ancaman atau berbagai ancaman
- **Titik asal serangan** - Jumlah titik di mana kejadian (serangan) tersebut berasal
- **Jumlah yang terlibat dalam serangan itu** - Berapa banyak sistem internal dan eksternal yang terlibat dalam kejadian (serangan) tersebut , dan berapa banyak sistem orang yang memiliki bobot pengaruh/kepentingan yang berbeda

- **Sumber Pengetahuan** - Kemampuan untuk melihat informasi yang berkaitan dengan salah satu ancaman tertentu melalui pengumpulan informasi secara online (Anda mungkin akan terkejut dengan apa yang dapat Anda temukan dengan sedikit proaktif)

3. Siklus hidup APT

Pelaku di balik advanced persistent threat menciptakan suatu risiko yang tumbuh dan berubah pada aset keuangan, kekayaan intelektual, dan reputasi organisasi dengan mengikuti proses yang berkesinambungan :

1. Menarget organisasi tertentu untuk tujuan tunggal
2. Mencoba untuk mendapatkan pijakan di lingkungan tersebut, taktik umum termasuk email *spear phishing* (percobaan *phishing* yang ditujukan langsung pada individu atau perusahaan tertentu).
3. Menggunakan sistem yang telah di-hack sebagai akses ke jaringan target
4. Menyebarkan alat tambahan yang membantu memenuhi tujuan serangan
5. Menutupi jejak untuk menjaga akses (masuk) di kemudian hari

Global APT dari semua sumber yang kadang-kadang disebut dalam bentuk tunggal sebagai APT, seperti referensi untuk pelaku di balik insiden atau serangkaian kejadian tertentu.
Pada 2013, Mandiant mempresentasikan hasil penelitian mereka pada serangan Cina yang diduga menggunakan metodologi APT antara 2004 dan 2013 yang diikuti siklus yang sama :

- Hack Awal - dilakukan dengan menggunakan *social engineering* dan *spear phishing*, melalui email, meng-gunakan virus zero-day (http://en.wikipedia.org/wiki/Zero-day_virus). Metode infeksi lain yang populer adalah menanam malware pada situs Web yang mungkin akan dikunjungi oleh pegawai (dari per-usahaan yang menjadi target).
- Menetapkan pijakan - menanam *software* administrasi jarak jauh dalam jaringan korban, membuat *backdoors* jaringan dan *tunnel* memungkinkan akses *stealth* pada infrastrukturnya.
- Tingkatkan *Privileges* - menggunakan eksploitasi dan password cracking untuk memperoleh hak administrator atas komputer korban dan memperluasnya ke akun administrator Windows.
- *Internal Reconnaissance* – mengumpulkan informasi tentang seputar infrastruktur, *trust relationship*, struktur domain Windows.
- Bergerak lateral - memperluas kontrol pada *workstation*, server, dan elemen infrastruktur dan melakukan panen data pada mereka.
- Menjaga Keberadaan - memastikan kontrol lanjutan atas saluran akses dan kepercayaan yang diperoleh pada langkah-langkah sebelumnya.
- Menyelesaikan Misi - *exfiltrate* (mengambil) data yang dicuri dari jaringan korban .

Dalam insiden yang dianalisis oleh Mandiant, periode rata-rata di mana para penyerang mengendalikan jaringan korban adalah satu tahun, dengan masa terpanjang - hampir lima tahun infiltrasi tersebut diduga dilakukan oleh Satuan 61398 Tentara Pembebasan Rakyat yang berbasis di Shanghai. Para pejabat Cina telah membantah ada keterlibatan apa pun dalam serangan ini .

4. Terminologi

Definisi APT yang tepat sangat bervariasi, tetapi dapat diringkas sesuai dengan namanya di bawah ini :

- ***Advanced*** - Operator di balik ancaman tersebut memiliki spektrum penuh teknik pengumpulan-intelijen. Hal tersebut termasuk teknologi dan teknik intrusi komputer, tetapi juga meluas ke teknik pengumpulan-intelijen konvensional seperti teknologi intersepsi-telepon dan pencitraan satelit. Sementara masing-masing komponen serangan itu tidak dapat digolongkan sebagai sangat "advanced" (misalnya komponen malware yang dihasil-kan dari do-it-yourself malware kit tersedia secara umum, atau penggunaan bahan exploitasi yang mudah diperoleh), operator-operator mereka dapat mengakses dan mengembangkan lebih banyak alat canggih yang diperlukan. Mereka sering mengga-

bungkan metode multiple penargetan, peralatan, dan teknik untuk mencapai dan meng-hack target mereka dan memperta-hankan akses ke sana. Operator juga menunjukkan fokus yang disengaja pada keamanan operasional yang membedakan mereka dari ancaman yang "kurang advanced" .

- ***Persistent*** - Operator mengutamakan tugas tertentu, bukan oportunis mencari informasi finansial atau lainnya. Perbedaan ini menunjukkan bahwa para penyerang dipandu oleh entitas eksternal. Penargetan ini dilakukan melalui pemantauan dan interaksi yang terus menerus dalam rangka mencapai tujuan yang telah ditetapkan. Hal ini tidak berarti rentetan serangan konstan dan update malware. Bahkan, pendekatan "*low-and-slow*" biasanya lebih berhasil. Jika operator kehilangan akses ke target mereka, mereka biasanya akan mencoba mengakses kembali, dan seringkali, berhasil. Salah satu tujuan operator adalah untuk menjaga akses jangka panjang pada target, berbeda dengan ancaman yang hanya memerlukan akses untuk menjalankan tugas tertentu.

- ***Threats*** - APT adalah suatu ancaman karena mereka memiliki keduanya, kemampuan dan niat. Serangan APT dijalankan oleh tindakan manusia yang terkoordinasi, bukan oleh satu kode/program yang ceroboh dan otomatis. Para operator memiliki tujuan tertentu dan mereka terampil , termotivasi, terorganisir dan didanai dengan baik .

5. Strategi mitigasi

Ada 100 juta variasi malware, yang membuatnya sangat menantang untuk melindungi organisasi dari APT. Sementara kegiatan APT yang tersembunyi dan sulit untuk dideteksi, komando dan kontrol lalu lintas jaringan yang terkait dengan APT dapat dideteksi pada tingkat lapisan jaringan. Analisis log yang mendalam dan korelasi log dari berbagai sumber dapat berguna dalam mendeteksi kegiatan APT - itu semua mengenai log. Agen dapat digunakan untuk mengumpulkan log (TCP dan UDP) langsung dari aset ke server syslog. Kemudian alat Security Information and Event Management (SIEM) dapat menghubungkan dan menganalisis log. Sementara hal itu menantang untuk memisahkan "suara" dari lalu lintas yang sah, alat korelasi log yang baik, seperti LogRhythm atau ArcSight dapat digunakan untuk menyaring lalu lintas yang sah, sehingga staf keamanan dapat fokus pada "suara" yang dicari/di ingin-kan[7].

6.2. Laporan tentang *Deface, Malware, Phising*

Ada laporan mengenai beberapa situs pernah terkena *deface*, *malware*, *phising*

Contoh situs yang pernah di-*deface*

- http://asrini.smkn1klaten.sch.id
- http://www.sman6bdg.sch.id/wh00t.htm
- http://www.smaracatur.sch.id/t6.htm
- http://smkn1tanggul.sch.id/zsn.php
- http://www.sman20bandung.sch.id/t6.htm
- http://www.smp1pandak.sch.id
- http://smkn3pandeglang.sch.id
- http://www.sdislambumiayu.sch.id/x.txt
- http://sdintegral-purwodadi.sch.id/index.php
- http://akademisiprestasi.dikti.go.id/dokumen/spy.html
- http://ijazahln.dikti.go.id/backup/v4/spy.html
- http://prodibaru.dikti.go.id/temp/spy.html

Contoh situs yang terkena *Malware*:

- |2014-04-10 14:41:25 CEST |24709223 |JS.Crypt-1 |103.247.8.124 http://sdn16btg.sch.id
- |2014-04-10 14:41:25 CEST |24709224 |JS.Crypt-1 |103.247.8.124 http://www.sdn5btg.sch.id
- (cleanmx_generic)http://afarsie.sman2solo.sch.id/thigh.html?lixubimuhu
- (Android-PUP/Hamob) http://www.smkn4jkt.sch.id/SMK%2BNegeri%2B4%2BJakarta.apk
- (JS/Redirector.aah) http://www.sekolah-pilar-indonesia.sch.id/library/spi-library-collection.html

[7] Sumber : wikipedia http://en.wikipedia.org/wiki/Advanced_persistent_threat

- (HTML/Rce.Gen3)
  http://www.smkpratiwiprabumulih.sch.id/html/guru.php?id=lihmateri
- (HTML/Drop.Agent.AB)
  http://bse.kemdiknas.go.id/buku/20080508115940
- (VBS_RAMNIT.SMC)
  http://bse.kemdiknas.go.id/buku/20080726143026/

Contoh situs yang terkena Phising

- http://maalishlah.sch.id/plugins/statmember/index.html
- http://smkmuh3kra.sch.id/ggggg/pp/home/
- http://pptkpaudni.kemdiknas.go.id/wp-content/gallery/galeri/thumbs/sbin.php
- Contoh beberapa IP Spam:
  - 118.98.164.42,
  - 118.98.232.50,
  - 118.98.162.106, dsb

- Network Incident/Brute Force

```
your Server/Customer with the IP: *118.98.172.188* has attacked one of our servers/partners. The attackers used the method/service: *bruteforcelogin* on: *Fri, 28 Jun 2013 05:53:25 +0200*.The attack was reported to the Blocklist.de-System on: *Fri, 28 Jun 2013 09:07:47 +0200*
```